IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

LIONRA TECHNOLOGIES LIMITED, v. FORTINET, INC.	Case No. 2:22-cv-00322-JRG-RSP (Lead Case) **JURY TRIAL DEMANDED** [redacted]
LIONRA TECHNOLOGIES LIMITED v. CISCO SYSTEMS, INC.	Case No. 2:22-cv-00305-JRG-RSP (Member Case)
LIONRA TECHNOLOGIES LIMITED v. PALO ALTO NETWORKS, INC.	Case No. 2:22-cv-00334-JRG-RSP (Member Case)

DEFENDANT CISCO SYSTEMS, INC.'S MOTION FOR PARTIAL SUMMARY JUDGMENT AS TO CISCO'S LICENSE DEFENSE AND NONINFRINGEMENT WITH RESPECT TO U.S. PATENT NOS. 7,685,436 AND 8,566,612

TABLE OF CONTENTS

Page

TABLE OF EXHIBITS

Exhibit	Document
Ex. 1	U.S. Patent No. 7,685,436
Ex. 2	U.S. Patent No. 8,566,612
Ex. 3	Patent License Agreement
Ex. 4	Excerpts of Rebuttal Expert Report on Noninfringement of Cisco's Technical Expert Dr. Kevin Jeffay
Ex. 5	Excerpts of Expert Report of Lionra's Technical Expert Dr. Hugh Smith
Ex. 6	Excerpts of Deposition Transcript of Cisco's 30(b)(6) Witness [redacted]
Ex. 7	Excerpts of Deposition Transcript of Lionra's Technical Expert Dr. Hugh Smith

TABLE OF AUTHORITIES

Page(s)

Cases

Cisco respectfully requests summary judgment of noninfringement as to claims 1 and 2 of U.S. Patent No. 7,685,436 (the "'436 patent") and claims 1, 2, and 12 of U.S. Patent No. 8,566,612 (the "'612 patent") (together the "Asserted Patents" and "Asserted Claims").

Lionra's infringement claim must fail because Cisco's Accused Products are licensed to the Asserted Patents. The Asserted Claims cover a security processor with a specific configuration of components, each of which includes hardware. For example, the Court construed—over Lionra's arguments otherwise—each of the claimed "packet engine," "cryptographic core," and "intrusion detection system" to require hardware. It is now undisputed that the hardware in the Cisco Accused Products that are alleged to satisfy at least the "packet engine" and "intrusion detection system" elements are Intel and AMD processors. Indeed, Lionra's expert conceded at deposition that the only hardware he accuses of infringing is the Intel and AMD processors in the Accused Products. [redacted]

Specifically, [redacted] Cisco's Accused Products are covered under both definitions.

[redacted]

[redacted]

[redacted].

In addition to the license defense, there is also no infringement because Lionra has failed to provide any evidence that the accused products are configured as claimed. In fact, the evidence Lionra relies on actually shows that the Accused Products operate contrary to what is claimed. Specifically, the claimed security processor must include an intrusion detection system ***coupled between*** the packet engine and the cryptographic core. This configuration was a key element added to the Asserted Claims during prosecution. However, Lionra has zero evidence that the alleged intrusion detection system is coupled between the alleged packet engine and the alleged cryptographic core. To the contrary, the evidence Lionra cites actually shows the opposite, that the alleged packet engine does initial packet classification, then passes the packet to the cryptographic core for decryption, and only then sends the packet to perform intrusion detection. Thus, if anything, the accused intrusion detection system is not "coupled *between*" the packet engine and cryptographic core but is instead coupled *after* the cryptographic core. Summary judgment of noninfringement should thus be granted on this basis.

I. STATEMENT OF ISSUES TO BE DECIDED BY THE COURT

A. Is there a dispute of material fact to whether the Accused Products are covered under the Patent License Agreement?

B. Is there a dispute of material fact as to whether what Lionra has identified as the accused intrusion detection system is coupled after the packet engine and cryptographic core, and not between them as the Asserted Claims require?

II. STATEMENT OF UNDISPUTED MATERIAL FACTS

1. Lionra asserts claims 1 and 2 of U.S. Patent No. 7,685,436 (the "'436 patent") and claims 1, 2, and 12 of U.S. Patent No. 8,566,612 (the "'612 patent") (together the "Asserted Patents" or "Asserted Claims"). Ex. 5, Smith Report at ¶ 12. The Asserted Claims are directed to a security processor having a switching system, a cryptographic core, and a packet engine for processing incoming and outgoing data packets that is ***interposed between*** the switching system and cryptographic core. *See, e.g.*, '436 patent at 24:33–34 (emphasis added). The Asserted Patents also claim an intrusion detection system using a signature database ***coupled between*** the packet engine and the cryptographic core. *Id.* at 24:35–39 (emphasis added). The configuration of these elements, and more specifically that the packet engine be interposed between the switching system and cryptographic core and that the intrusion detection system be coupled between the packet engine and the cryptographic core were added to the Asserted Claims during prosecution in response to rejections by the examiner. [redacted] (citing April 27, 2009 Response and Amendment and July 30, 2004 Amendment to Claims in Response to Nonfinal Rejection during '436 Patent Prosecution History); [redacted]

[redacted] Cisco's expert provides undisputed testimony that at least the "packet engine" and "intrusion detections system" limitations are material to the claims. Ex. 4, Jeffay Report at ¶ 69.

2. At claim construction, Lionra argued that the terms "packet engine," "cryptographic core" and "intrusion detection system" did not require hardware, and could instead be satisfied merely by software. *See, e.g.*, Dkt. No. 162 at 35, 40, 44. The Court rejected Lionra's argument, and entered the below constructions, confirming that each of these claim elements must include at least hardware:

Claim Term	**Court's Construction**
"packet engine"	"hardware, or a combination of hardware and software, that is configured to perform packet operations."
"cryptographic core"	"hardware, or a combination of hardware and software, that is configured to perform cryptographic processing."
"intrusion detection system"	"hardware, or a combination of hardware and software, that is configured for matching parts of a data stream against a stored set of patterns."

Id. at 39 42, 46.

3. The Accused Products are Cisco firewalls that run Cisco's Firepower Threat Defense firewall software. [redacted] More specifically, Lionra accuses the following models of Cisco firewalls running Cisco Firepower Threat Defense software: Firepower 1010, 1120, 1140, 1010E, 1150, 2110, 2120, 2130, 2140, 4110, 4120, 4140, 4150, 4115, 4125, 4145, 4112, 9300, SM-24, SM-36, SM-44, SM-40, SM-48, SM-56; Secure Firewall 3105, 3110,

3120, 3130, 3140, 4215, 4225, 4245; ISA 3000; ASA 5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X (collectively "Accused Products").[1]

4. It is undisputed that Cisco is a customer of Intel and AMD and that each Accused Product includes at least one Intel or AMD processor. [redacted] It is also undisputed that the Intel or AMD processors in each Accused Product are identified as satisfying at least the "packet engine" and "intrusion detection systems" elements. [redacted] For [redacted]

5. [redacted]

[1] During discovery, Lionra had accused only Firepower Management Center products of infringement. *See* Dkt. No 223. On the last day of discovery, Lionra moved to amend its infringement contentions to replace the list of accused products with the list set forth in this paragraph. Dkt. No 197. On February 2, 2024, the Court granted Lionra's motion. Dkt. No 240.

[redacted]

[redacted] [redacted]

> [redacted]

[redacted]

> [redacted]

> [redacted]

[redacted]

> [redacted]

[redacted]

> [redacted]

III. ARGUMENT

A. The Cisco Accused Products are Licensed Under the Patent License Agreement

Lionra fought hard to avoid a construction of the Asserted Claims that requires hardware. Despite Lionra's best efforts, the Court unambiguously required that the key elements of the

Asserted Claims (namely the "packet engine," "cryptographic core" and "intrusion detection system") all require "hardware, or a combination of hardware and software." SUMF 2. In addition, despite accusing a different set of products throughout the case, Lionra was permitted to change its infringement allegations to accuse Cisco firewall products of infringing the Asserted Claims. SUMF 3. While that 180-degree shift in infringement allegations allowed Lionra to proceed with its case, it landed Lionra in an untenable predicament in view of the Court's claim construction. [redacted]

[redacted].

Under Delaware law, [redacted] contract interpretation is a question of law. *See JFE Steel Corp. v. ICI Americas, Inc.*, 797 F. Supp. 2d 452, 469 (D. Del. 2011) (citing *Rhone–Poulenc Basic Chems. Co. v. American Motorists Ins. Co.,* 616 A.2d 1192, 1195 (Del. 1992). Here, the issue before the Court is a pure question of contract interpretation. [redacted]

[redacted]

[redacted]

> [redacted]

[redacted] *See De Forest Radio Telephone & Telegraph Co. v. United States*, 273 U.S. 236 (1927) (holding that in the context of a patent infringement action a covenant not to sue constituted a license); *see also TransCore, LP v. Electronic Transaction Consultants Corp*., 563 F.3d 1271 (Fed. Cir. 2009).

The Accused Products are also covered under the definition of [redacted] [redacted] [redacted] is defined to include [redacted]

[redacted]

[redacted]

[redacted]

[2] [redacted]

no dispute that the elements ("packet engine" and "intrusion detection system") are material to the claims. [redacted] [redacted] [redacted] Indeed, the intrusion detection system, and its relationship to the other hardware components in the claims, were added during prosecution to avoid prior art rejections. SUMF 1.

Accordingly, because [redacted] and Lionra's infringement allegations are foreclosed as a matter of law.

B. The Accused Products Do Not Infringe Because the Intrusion Detection System is Coupled At Best After the Packet Engine and Cryptographic Core, not Between Them as the Claims Require

Each Asserted Claim requires "an intrusion detection system ***coupled between*** the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database." *See, e.g.*, '436 Patent at 36–39. Fig. 3 and the description of Fig. 3 in the shared specification of the Asserted Patents depicts this configuration in which the intrusion detection system is between the packet engines and cryptographic cores. '436 Patent at Fig. 3, 18:41–57.

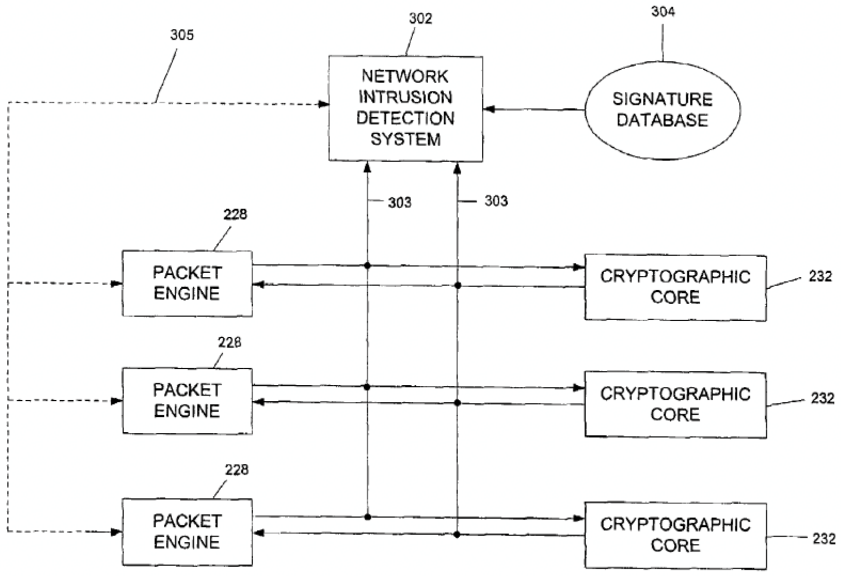

FIG. 3

The intrusion detection limitation, and the requirement that it be coupled between the packet engine and cryptographic core, was first added to the Asserted Claims during the prosecution of the ’436 Patent to overcome a rejection by the Examiner, and this configuration of elements was material to the allowance of the claims. [redacted] The limitation was carried through to the claims of the ’612 Patent. *Id.*

Lionra bases its infringement arguments purely on the flow of data packets through the system, rather than pointing to components and how they are coupled to each other. *See, e.g.*, [redacted] That alone dooms Lionra’s case, since the claims require a specific coupling arrangement. But even taking Lionra’s allegations on their face, Lionra identifies an entirely different arrangement of components than what is claimed. Namely, all of the evidence Lionra provides shows that the software components it identifies as satisfying the claims are configured in an order that has the intrusion detection system *coupled after* the packet engine and cryptographic core, not between them, as the claims require.

While Dr. Smith provides unsupported statements that the accused intrusion detection system is coupled between the packet engine and cryptographic core, all evidence cited is to the contrary. Thus, the Court should give little to no weight to his unsupported opinion. *See, e.g.*, *McIntosh v. Partridge,* 540 F.3d 315, 322 (5th Cir. 2008). More specifically, all evidence Lionra cites regarding the packet flow in the accused Firepower Threat Defense software shows that the alleged packet engine does initial packet classification, then the packet is passed to the cryptographic core for decryption, and then once decrypted, intrusion detection is performed on the decrypted packet. [redacted] [redacted] In other words, the evidence Lionra cites showing the data flow in the accused products demonstrates that the packet engine is coupled after the cryptographic core and packet engine, not between them. *Id.*

[redacted]

[redacted]

[redacted] For further example, the technical document describing the Accused Products, titled Network Analysis and IPS overview, repeatedly cited by Dr. Smith, shows intrusion detection policies (green) being enforced after decryption (red):

[redacted]

[redacted]

In other words, all of the evidence Lionra cites shows that the accused intrusion detection system is coupled ***after*** the packet engine and cryptographic core.[3] This flow is consistent with the description of the functionality from Cisco's 30(b)(6) witness and Cisco's technical expert. [redacted] And more specifically, both Cisco and Lionra's witnesses explain the need for initial classification, then to decrypt the packet in order to be able to view its contents before packets are inspected for intrusions. [redacted] [redacted]

Accordingly, there is no dispute of material fact as to whether the Accused Products satisfy the "coupled between" requirement of the "an intrusion detection system coupled between the

[redacted]

cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database" claim element because it is indisputable that the accused intrusion detection system in the Accused Products is coupled, if at all, ***after*** both the packet engine and cryptographic core.

IV. CONCLUSION

For the foregoing reasons, Cisco respectfully requests that the Court grant summary judgment as to Cisco's license defense and noninfringement with respect to the Asserted Claims of the '436 and '612 Patents.

Dated: February 20, 2024

/s/ Brian A. Rosenthal

Brian A. Rosenthal (lead attorney)
brosenthal@gibsondunn.com
Katherine Dominguez
kdominguez@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.6300
Facsimile: 212.351.4035

Stuart M. Rosenberg
srosenberg@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1881 Page Mill Road
Palo Alto, CA 94304-1211
Telephone: 650.849.5300
Facsimile: 650.849.5333

Albert Suarez IV
asuarez@gibsondunn.com
Texas State Bar No. 24113094
GIBSON, DUNN & CRUTCHER LLP
2001 Ross Avenue, Suite 2100
Dallas, TX 75201-6912
Telephone: 214.698.3360
Facsimile: 214.571.2907

Melissa R. Smith
melissa@gillamsmithlaw.com
Texas State Bar No. 26301351
GILLAM & SMITH, LLP
303 South Washington Avenue
Marshall, Texas 75670
Telephone: 903.934.8450
Facsimile: 903.934.9257

Attorneys for Defendant Cisco Systems, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on February 20, 2024, the foregoing was electronically filed with the Clerk of the Court using the CM/ECF system and served on all counsel of record by electronic mail on this 20th day of February 2024.

/s/ Brian A. Rosenthal
Brian A. Rosenthal

CERTIFICATE OF AUTHORIZATION TO SEAL

I hereby certify that pursuant to the protective order the above-captioned case, this motion and exhibits hereto contain confidential information. Accordingly, this document is to be filed under seal.

/s/ Brian A. Rosenthal
Brian A. Rosenthal